FIG. 1

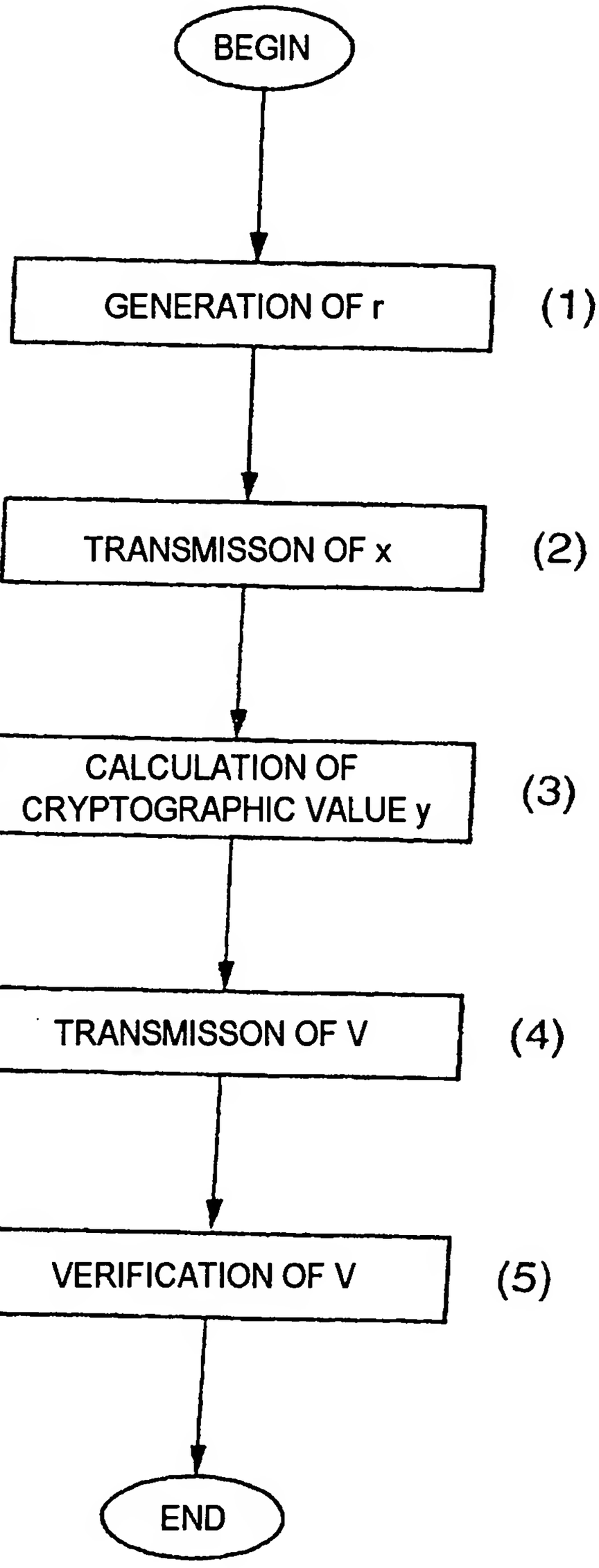

BEGIN
GENERATION OF r
(1)
TRANSMISSON OF x
(2)
CALCULATION OF CRYPTOGRAPHIC VALUE y
(3)
TRANSMISSON OF V
(4)
VERIFICATION OF V
(5)
END

FIG. 2

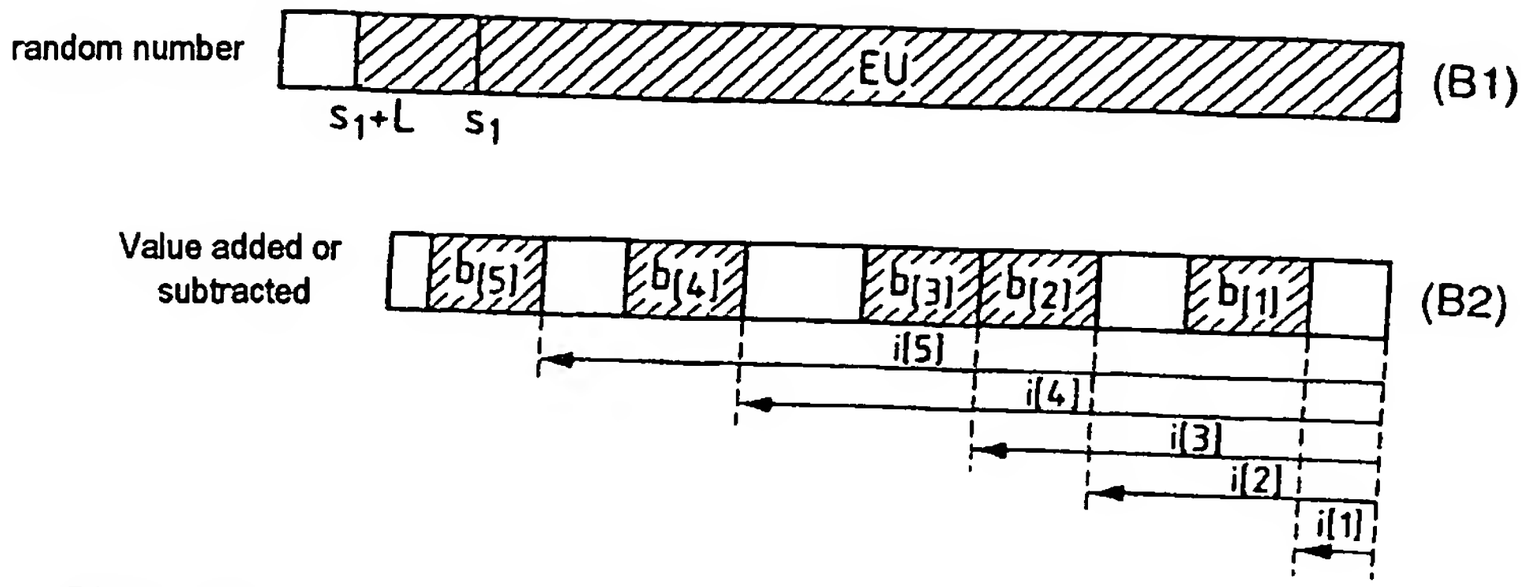


FIG. 3

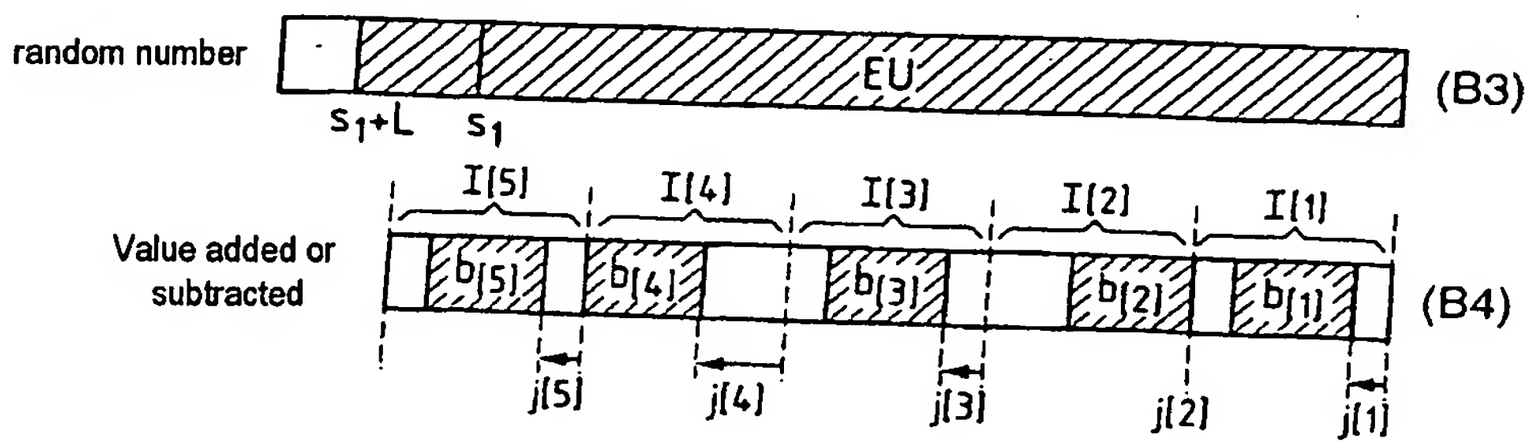


FIG. 4

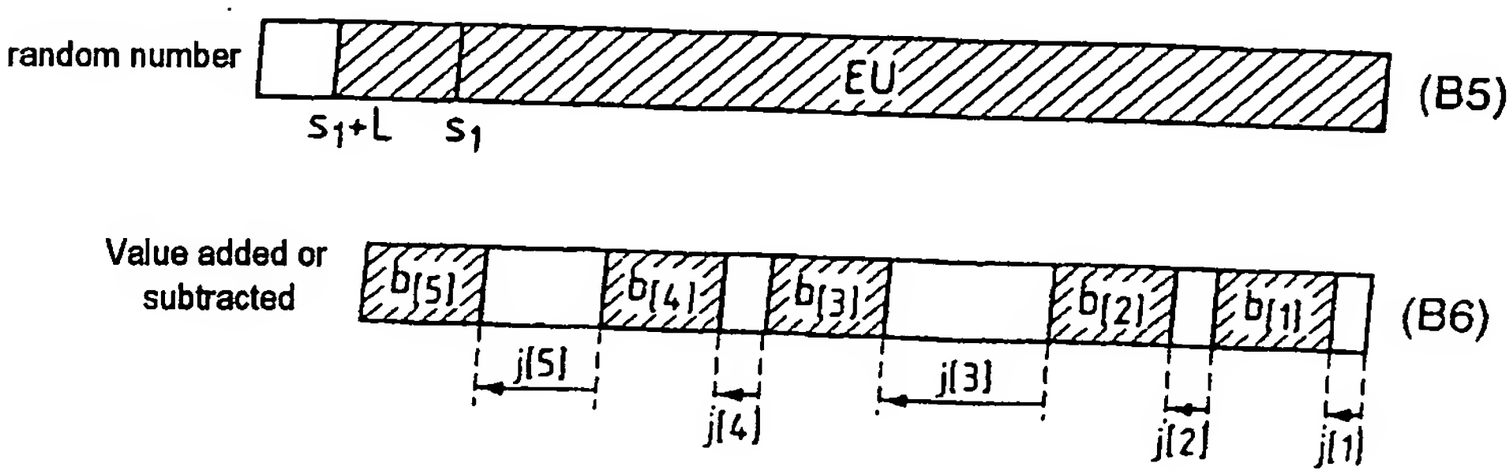


FIG. 5

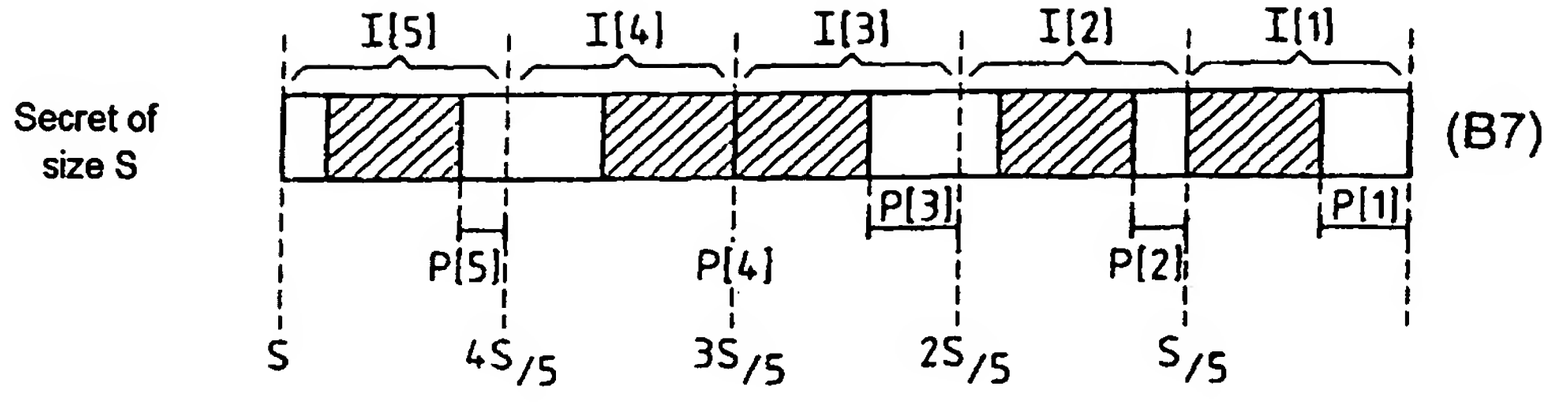
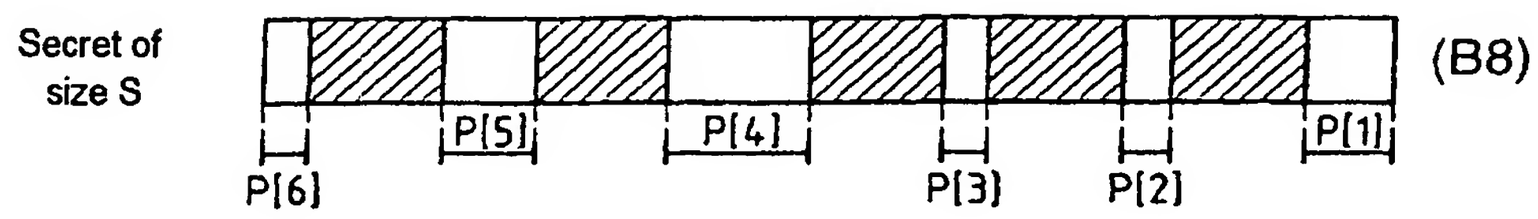

Secret of size S
I[5]
I[4]
I[3]
I[2]
I[1]
(B7)
P[5]
P[4]
P[3]
P[2]
P[1]
S
4S/5
3S/5
2S/5
S/5

FIG. 6


Secret of size S
(B8)
P[6]
P[5]
P[4]
P[3]
P[2]
P[1]

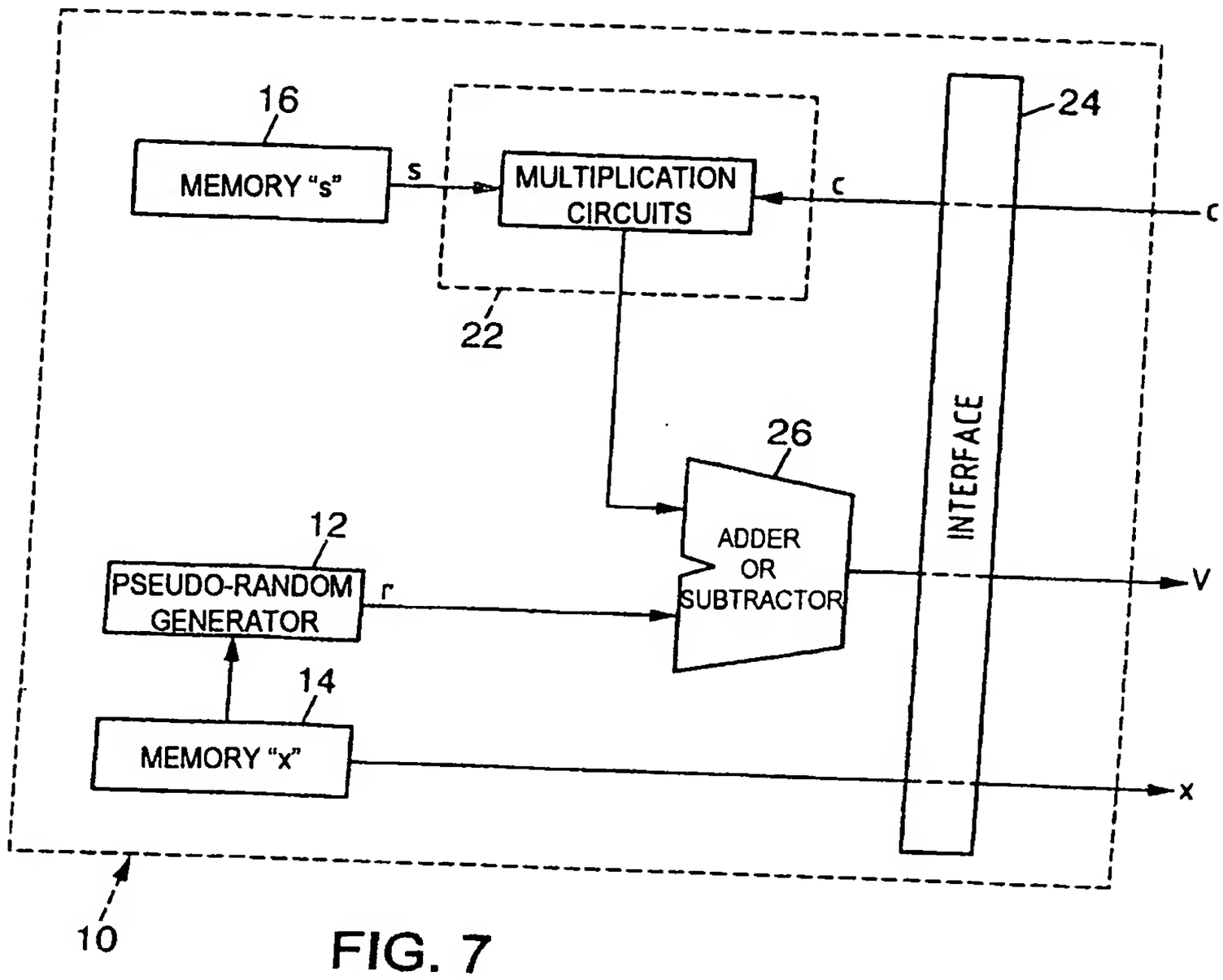

16
MEMORY "s"
s
MULTIPLICATION CIRCUITS
c
c
24
22
26
INTERFACE
ADDER OR SUBTRACTOR
V
12
PSEUDO-RANDOM GENERATOR
r
14
MEMORY "x"
x
10

FIG. 7

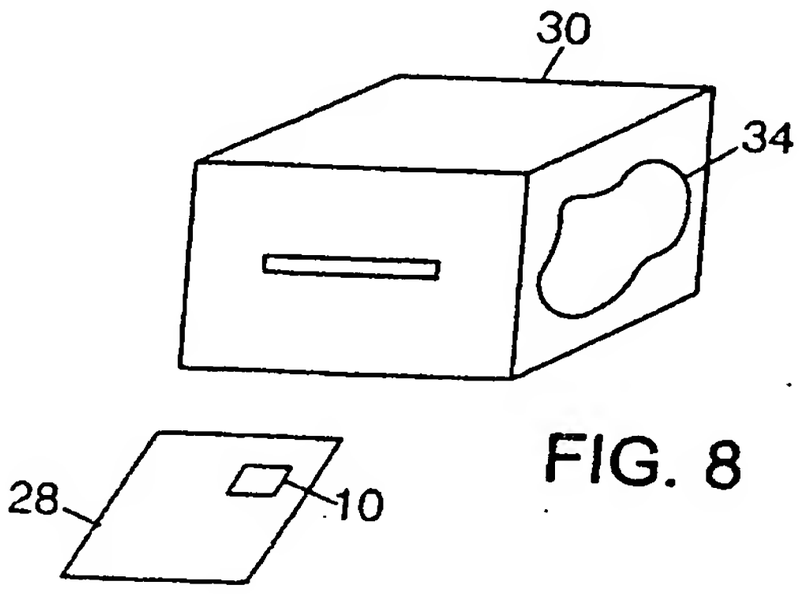

30
34
28
10

FIG. 8